International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

A COMPARATIVE ANALYSIS OF SYMMETRIC AND ASYMMETRIC KEY CRYPTOGRAPHY

Naveen Kumar R[1], Poovarasan R[2], Saravana Harish S[3], Jagadish D[4]

[1] *School of Information Technology & Engineering,VIT University,Tamilnadu,India.*
[2] *School of Information Technology & Engineering,VIT University,Tamilnadu,India.*
[3]*School of Information Technology & Engineering,VIT University,Tamilnadu,India.*
[4]*School of Information Technology & Engineering,VIT University,Tamilnadu,India.*

Abstract - Arrange protection procedures start and execution is significant with the end goal of secured information transmission and privacy. Cryptography is a strategy which is produced exclusively with the end goal of information security and trustworthiness during the time spent correspondence. Despite the fact that few speculations and ideas exists, each changes with the measure of security it offers to the system channel. An imperative component which decides the kind of cryptography is key circulation. In light of the kind of key appropriation, cryptography is Comprehensively delegated symmetric and uneven. In this paper, the established calculations which are utilized for symmetric and awry cryptography.

Key Words: Public and Private Key, Encryption, Decryption.

1.INTRODUCTION

Cryptography is the strategy of scrambling plain content. This secures information and data from any inward or outer assaults. In this manner, it gives uprightness, classification;
non-renouncement and credibility to the mystery data. The writings required in cryptography are plain and figure writings. Plain messages are intelligible writings and the data which the sender means to send. The plain content is encoded to an obscured frame called the figure text. Based on the encryption strategy utilized, it is separated as symmetric and lopsided cryptography.
Current cryptography worries about the accompanying four destinations:

- Concealment-unintended individual can't block the message.
- Uprightness-no change is allowed between the sender and recipient.
- Nonrepudiation-the sender of the message can't differ at a later stage his goals really taking shape of the data.
- Authentication-the affirmation of sender's and collector's personality can be performed by each other.

SYMMETRIC KEY CRYPTOGRAPHY:

Symmetric key cryptography is likewise called mystery key or shared key cryptography. In this sort of cryptography, the sender and beneficiary share a typical key for both
encryption and decoding. The enter utilized as a part of this strategy is ensured without anyone else. The key is shared through correspondence. On the off chance that an interloper gets the key, the entire procedure is traded off and the gatecrasher can without much of a stretch unscramble
the message. This strategy is favored on account of its quick administration and less asset prerequisite. The calculations looked at in this paper are DES, 3DES, AES, BLOWFISH, RC2,

RC4, SKIPJACK.

ASYMMETRIC KEY CRYPTOGRAPHY:

The asymmetric key cryptography is otherwise called open key cryptography. Scrambling of content is completed utilizing open key of the sender and translating is doneutilizing the private key of the collector. The idea of self-accreditation is missing here on the grounds that advanced marks are utilized to bear witness to the keys. This technique gives better validation and security as the protection stays in place. There are different calculations to execute this cryptography system. They are RSA, Diffie-Hellman, ECC and Digital Signature Algorithm,
Rabin, EIGamal.

COMPARATIVE ANALYSIS OF TRADITIONAL CRYPTOGRAPHY ALGORITHMS:

Customary calculations are the current strategies utilized for accomplishing the procedure of cryptography. These calculations are very much tried before they are being actualized in an application. Each calculation contrasts with the each other on different terms. In light of the test outcomes, the accompanying (table 1) is inferred in view of the course of action, key measurements, number of rounds, and figure sort.

TABLE 1:

Method	Arrangement	No of rounds	Key dimension	Type
DES	Balanced Fiestel-Network	16	56	Chunk
3DES	Fiestel-Network	48	112,168	Chunk
RC2	Source-Heavey Fiestel-Network	18	40 to 1024	Chunk
RC4	Nil	256	40 to 20488	Stream
AES	Substitution Permutation Network	10,12,14	123,192,256	Chunk
BLOWFISH	Fiestel-Network	16	32 to 448	Chunk
SKIPJACK	Unbalanced Fiestel-Network	32	80	Chunk

ENCRPTION TIME FOR FLV AND BMP FILE TYPES:

Each document sets aside its own particular time for encryption as for its sort and size. The most widely recognized record sorts utilized are BMP and FLV. Each calculation perform at an alternate pace since they vary with the quantity of rounds in encoding the source message.

The accompanying table (table.2) is inferred as the consequence of dissecting the time taken for a specific record through a particular calculation.

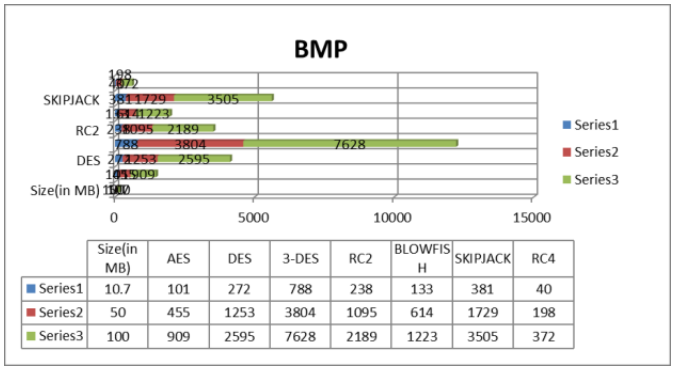
TABLE 2:

FILE TYPE	SIZE IN (MB)
DES	56
3DES	112
RC2	40
RC4	40
AES	128
BLOWFISH	32
SKIPJACK	80

GRAPHICAL REPRESENTATION OF ENCRYPTION TIME TAKEN:

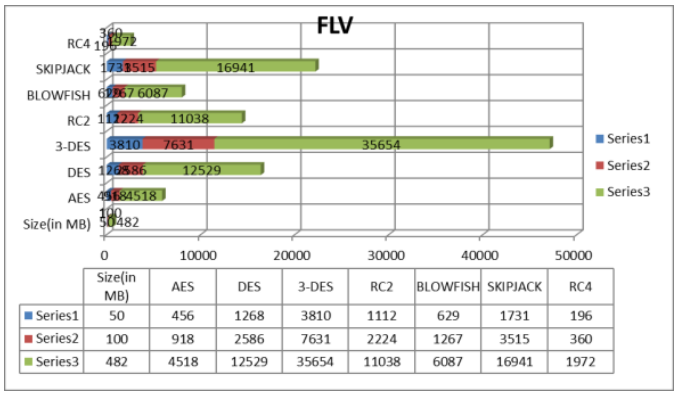
The qualities gave in the table is spoken to as a chart for the simple translation of the induction. Two separate charts are drawn for two record sorts. The x-pivot speaks to the measure
of the picture document while the y-hub speaks to the sort of calculation. The authoritative point is to know the speed of every technique when playing out the encryption. Fig.1, demonstrates the time taken for scrambling BMP record and Fig.2, demonstrates the time taken for encoding FLV document.

FIGURE 1:



	Size(in MB)	AES	DES	3-DES	RC2	BLOWFISH	SKIPJACK	RC4
Series1	10.7	101	272	788	238	133	381	40
Series2	50	455	1253	3804	1095	614	1729	198
Series3	100	909	2595	7628	2189	1223	3505	372

FIGURE 2:



	Size(in MB)	AES	DES	3-DES	RC2	BLOWFISH	SKIPJACK	RC4
Series1	50	456	1268	3810	1112	629	1731	196
Series2	100	918	2586	7631	2224	1267	3515	360
Series3	482	4518	12529	35654	11038	6087	16941	1972

COMPARATIVE STUDY OF ASYMMETRIC KEY ALGORITHMS:

This sort of technique requires combine of keys to fulfill the motivation of encryption and unscrambling. The key match is normally numerically identified with each other. When one key scrambles, the other one must be utilized to translate the content. The distinctive calculations utilized for uneven key cryptography are quickly clarified beneath.

RIVEST-SHAMIR-ADLEMAN (RSR):

General equation is (d, e) where d means the private key and e symbolizes the general population key. Both encryption and unscrambling utilizes a similar capacity. It is exceedingly
secure in light of the fact that it is hard to create the private key from the general population key and modulus. The assailants think that it's hard to process the turnaround of e. Many-sided quality of creating the key is high. The procedure of cryptography is very moderate. It has not been tried that it is equal to the factorization technique and it is repetitive to factorize substantial

numbers. The key length ought to be bigger than 1024 bits.

RABIN:

It is utilized for Integer factorization issue, Square roots modulo composite. Rabin is secure against assaults by inactive enemy and inconceivably quick because of single module squaring. Slower decoding strategy contrasted with RSA technique. It is very defenseless against RSA assaults.

ELLIPTICAL CURVE CRYPTOGRAPHY (ECC):

Elliptic bend conditions are utilized to process the keys. It can give security utilizing a 164 piece key and has a greater number of preferences than RSA and Diffie Hellman
calculations. The power abuse is low and gives better advantages to batteries. Size of encoded message is expanded and the execution is exceptionally troublesome because of the high many-sided quality contrasted with RSA. Elliptic Curve Digital Signature Algorithm (ECDSA) is acquainted with fills this need. The Authenticated key assention convention, ECMQV secures the framework against man in the center assaults.

DIGITAL SIGNATURE ALGORITHM (DSA):

Information verification is done utilizing a couple of vast numbers processed utilizing a few calculations. Private keys are utilized to create marks and open keys are utilized to check them. It is quick and gives non-revocation and authenticity. It ensures the information against various assaults like Man-in-the-Middle assaults and has a bigger number of preferences than other customary topsy-turvy key calculations. Advanced marks have short life expectancy. They muddle sharing since they are not good. Confirmation programming is fundamental. Computerized endorsements ought to just be purchased from confided in specialists.

DIFFIE-HELLMAN:

It depends on the sharing of mystery cryptographic key. This key is utilized for both encryption and decoding purposes. It relies on upon hardness of the discrete logarithms. The
calculation is very quick since the symmetric key is of short length (256 bits). The assaults raises with the use of symmetric keys. This calculation is more defenseless against Man in the Middle assaults. Visit key changing is vital. Improvement of Station-to-Station behavior ousts Man in
the Middle assaults. The advance of computerized mark is additionally an answer for the assaults.

EIGAMAL:

It depends on discrete logarithm issue, Diffie-Hellman issue. It utilizes randomization encryption. Plain content is a large portion of the measure of figure content. Element of two
unequivocally adaptable along these lines inclined to picked figure content assault. There exists a
plausibility of false marks. It can be broken in the event of frail choice of p and e. Encryption is moderate as it includes two measured exponentiations.

CONCLUSION:

Both Symmetric and Asymmetric Key calculations are exceedingly able in securing the exchanged information over any correspondence medium. In this paper, the customary
calculations are talked about. Symmetric cryptography uses a solitary key to accomplish encryption and decoding which could rise security issues. Then again, Asymmetric Key Cryptography utilizes two separate keys to keep any exploitative access to the information. One key stays private while the other is accessible in people in general key vault. The last gives more security than the previous. Still symmetric cryptographic systems are favored for their less
complex depiction and less prerequisite of assets. In future, for creative and secured information transmission, cryptography is an extreme arrangement. Different applications can be constructed utilizing symmetric and awry calculations for upgrading the assurance. The higher the securities of the framework, lesser are the odds of breaking into it. The fate of security framework relies on
upon such calculations which make the interruption completely inconceivable.

REFERENCES:

[1]Adam J, Elbert and Christof Paar, an Instruction-Level Distributed Processor for Symmetric-Key Cryptography, IEEE Transactions on Parallel and Distributed Systems, 16 (5), 2005, 468-480.

[2]Ankita Baheti, Lokesh Singh, and Asif Ullah Khan,Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System and Authentication using Neural Network, Fourth International Conference on Communication Systems and Network Technologies, IEEE,
2014, 664-668 .

[3]Ankur Chaudhary, Khaleel Ahmad, and Rizvi M.A, E-commerce Security through Asymmetric Key Algorithm, Fourth International, 2014.

[5]Bibhudendra Acharya, Sambit Kumar Shukla, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda,H-S-X Cryptosystem and Its Application to Image Encryption, 2009